

МИНОБРНАУКИ РОССИИ



Федеральное государственное бюджетное образовательное учреждение
высшего образования

«Российский государственный гуманитарный университет»

(ФГБОУ ВО «РГГУ»)

ИНСТИТУТ ИНФОРМАЦИОННЫХ НАУК И ТЕХНОЛОГИЙ БЕЗОПАСНОСТИ

ФАКУЛЬТЕТ ИНФОРМАЦИОННЫХ СИСТЕМ И БЕЗОПАСНОСТИ

Кафедра комплексной защиты информации

***ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ
И ЗАЩИТА ИНФОРМАЦИИ***

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Направление и код подготовки - 46.03.02 «Документоведение и архивоведение»

Направленность (профиль) – Делопроизводство в организациях

Уровень квалификации выпускника (бакалавр)

Форма обучения очная

РПД адаптирована для лиц
с ограниченными возможностями
здоровья и инвалидов

Информационная безопасность и защита информации

Рабочая программа дисциплины

Составитель(и):

Старший преподаватель кафедры КЗИ Г.Н. Гудов

Ответственный редактор

Доктор технических наук, старший научный сотрудник, зав. кафедрой КЗИ О.В. Казарин

УТВЕРЖДЕНО

Протокол заседания кафедры

комплексной защиты информации

№ 1 от 29.08.2018 г. _____

ОГЛАВЛЕНИЕ

1. Пояснительная записка

1.1 Цель и задачи дисциплины

1.2. Формируемые компетенции, соотнесённые с планируемыми результатами обучения по дисциплине

1.3. Место дисциплины в структуре образовательной программы

2. Структура дисциплины

3. Содержание дисциплины

4. Образовательные технологии

5. Оценка планируемых результатов обучения

5.1. Система оценивания

5.2. Критерии выставления оценок

5.3. Оценочные средства (материалы) для текущего контроля успеваемости, промежуточной аттестации обучающихся по дисциплине

6. Учебно-методическое и информационное обеспечение дисциплины

6.1. Список источников и литературы

6.2. Перечень ресурсов информационно-телекоммуникационной сети «Интернет»

7. Материально-техническое обеспечение дисциплины

8. Обеспечение образовательного процесса для лиц с ограниченными возможностями здоровья

9. Методические материалы

9.1. Планы самостоятельных, практических, лабораторных занятий

9.2. Методические рекомендации по подготовке письменных работ (рефератов, докладов)

Приложения

Приложение 1. Аннотация дисциплины

Приложение 2. Лист изменений

1. Пояснительная записка

1.1. Цель и задачи дисциплины

Цель дисциплины:

изучение теоретических и прикладных вопросов информационной безопасности и защиты информации в сфере документооборота и архивного дела в Российской Федерации.

Задачи дисциплины:

изучить исторические этапы развития информационной безопасности и защиты информации;

освоить терминологию и понятийный аппарат в области информационной безопасности и защиты информации;

изучить нормативно-правовую базу, регулирующую сферу информационной безопасности и защиты информации; изучить основные средства и методы обеспечения информационной безопасности;

научить определять угрозы, уязвимости и риски информационной безопасности; обучить навыкам защиты информации;

научить применять полученные знания и навыки по информационной безопасности и защите информации в сфере документооборота и архивного дела.

1.2. Формируемые компетенции, соотнесенные с планируемыми результатами обучения по дисциплине

Дисциплина направлена на формирование следующих компетенций:

способностью использовать теоретические знания и методы исследования на практике (ОПК -1)		
Владение	Умение	Знание
терминологией и понятийным аппаратом в области информационной безопасности и защиты информации	определять угрозы, уязвимости и риски информационной безопасности	нормативно-правовую базу обеспечения информационной безопасности и защиты информации
владением базовыми знаниями в области информационных технологий (программные продукты, используемые в управлении документами, системы электронного документооборота, технологии сканирования документов) (ОПК-2)		
Владение	Умение	Знание
терминологией и понятийным аппаратом в области информационной безопасности и защиты информации	– анализировать проблемы информационной безопасности и защиты информации в системах документооборота и архивном деле	систему документационного обеспечения информационной безопасности и защиты информации

1.3. Место дисциплины в структуре основной образовательной программы

Дисциплина «Информационная безопасность и защита информации» относится к блоку Б1 дисциплин базовой части учебного плана.

Для освоения дисциплины необходимы компетенции, формируемые в ходе изучения дисциплин: «Информатика» «Вычислительные системы, сети и телекоммуникации», «Информационные системы» «Информационные технологии».

В результате освоения дисциплины формируются компетенции, необходимые для изучения следующих дисциплин: «Разработка и внедрение информационных систем», «Управление проектами информационных систем».

2. Структура дисциплины

(2017,2018 год)

Общая трудоемкость дисциплины составляет 2 зачетные единицы, 72 часов, в том числе контактная работа 28 часов, самостоятельная работа 44 часа.

№ п/п	Раздел дисциплины/темы	Семестр	Виды учебной работы (в часах)						Формы текущего контроля успеваемости, форма промежуточной аттестации (по семестрам)
			контактная					Самостоятельная работа	
			Лекции	Семинар	Практические занятия	Лабораторные занятия	Промежуточная аттестация		
1.	Методологические аспекты информационной безопасности и защиты информации	5	2	---	---	---	---	8	
1.1.	Введение в дисциплину	5	1	---	---	---	---	4	Устный опрос по теме.
1.2.	Базовые угрозы информационной безопасности	5	1	---	---	---	---	4	Устный опрос по теме.
2.	Информационная безопасность. Меры обеспечения информационной безопасности	5	4	---	---	8	---	12	
2.1.	Законодательный уровень обеспечения информационной безопасности	5	1	---	---	---	---	3	Устный опрос по теме. Доклад по теме.
2.2.	Административный уровень, цели, задачи, управление рисками	5	1	---	---	---	---	3	Устный опрос по теме. Доклад по теме.
2.3.	Процедурный уровень, назначение, основные	5	1	---	---	---	---	3	Устный опрос по теме.

	направления и принципы организации работ								Доклад по теме.
2.4.	Программно-технический уровень обеспечения информационной информации	5	1	---	---	8	---	3	Устный опрос по теме. Подготовка и выполнение лабораторной работы №1.
3.	Система защиты информации	5	4	---	---	8	---	12	
3.1.	Основные положения по организации защиты информации	5	2	---	---	---	---	6	Устный опрос по теме. Доклад по теме.
3.2.	Порядок построения системы защиты информации	5	2	---	---	8	---	6	Устный опрос по теме. Подготовка и выполнение лабораторной работы №2.
4.	Контроль и ответственность по обеспечению информационной безопасности и защиты информации	5	2	---	---	---	---	12	
4.1.	Контроль состояния режима безопасности и защиты информации	5	1	---	---	---	---	6	Устный опрос по теме. Доклад по теме.
4.2.	Ответственность за правонарушения и преступления в области информационной безопасности и защиты информации	5	1	---	---	---	---	6	Устный опрос. По теме. Доклад по теме
5.	Промежуточная аттестация (зачет)	5	---	---	---	---			Зачет по билетам
	Итого:		12			16		44	

3. Содержание дисциплины

Раздел 1. Методологические аспекты информационной безопасности и защиты информации

Тема 1. Введение в дисциплину

Понятие безопасности объекта (государства, предприятия и информационной системы). Основные компоненты безопасности государства и доминирующая роль информационной безопасности (ИБ). Становление и развитие понятия «информационная безопасность». Сущность и понятия ИБ и защиты информации. Необходимость и значение нормативно-

правового определения основных понятий. Связь ИБ с информатизацией общества. Базовые уровни обеспечения информационной безопасности и защиты информации.

Тема 2. Базовые угрозы информационной безопасности

Классификация угроз безопасности по цели реализации угрозы, принципу, характеру и способу её воздействия. Особенности угроз воздействия на объект атаки в зависимости от его состояния и используемых средств атаки. Основные методы и каналы несанкционированного доступа к информации в ИС. Базовые принципы защиты от несанкционированного доступа к информации в соответствии с нормативно-правовыми документами России. Задачи по защите информационных систем от реализации угроз.

Раздел 2. Информационная безопасность. Меры обеспечения информационной безопасности

Тема 3 Законодательный уровень обеспечения информационной безопасности

Предпосылки создания международных и российских стандартов по обеспечению информационной безопасности.

Назначение и основные положения международных стандартов: «Критерии оценки надежности компьютерных систем» («Оранжевая книга»), «Информационная безопасность распределенных систем. Рекомендации X.800», ISO 15408 – «Общие критерии». Международные стандарты семейства 27000.

Государственная система по обеспечению безопасности и защиты информации (ГСЗИ). Основные законодательные акты РФ в области информационной безопасности и защиты информации. Руководящие документы ФСБ, ФСТЭК России в области информационной безопасности и защиты информации от несанкционированного доступа при ее обработке с использованием СВТ.

Тема 4. Административный уровень, цели, задачи, управление рисками

Концепция информационной безопасности (ИБ), её цели и этапы построения. Политика и программа информационной безопасности, как основа административных мер по защите информации на предприятии. Структура документа, характеризующего политику и программу информационной безопасности. Анализ и управление рисками для ИС. Базовые методики, используемые для оценки рисков. Базовые инструментальные средства для анализа рисков и управления рисками.

Тема 5. Процедурный уровень, назначение, основные направления и принципы организации работ

Назначение и задачи процедурного уровня по обеспечению информационной безопасности. Основные классы мер процедурного уровня: управление персоналом,

физическая защита, поддержание работоспособности, реагирование на нарушения режима безопасности, планирование восстановительных работ.

Тема 6. Программно-технический уровень обеспечения информационной информации

Основные понятия программно-технического уровня обеспечения информационной безопасности. Особенности современных информационных систем, существенные с точки зрения обеспечения информационной безопасности. Архитектурная безопасность.

Программные сервисы защиты информации в информационных системах. Идентификация и аутентификация пользователей. Базовые методы парольной аутентификации. Модели разграничения доступа к информации. Протоколирование и аудит (активный и пассивный) информационной системы, их основные цели и особенности. Базовые методы криптографического преобразования данных. Процедура формирования электронной подписи. Экранирование информации в сетях. Компьютерные вирусы и вредоносные программы: классификация, методы и средства борьбы с ними.

Раздел 3. Система защиты информации

Тема 7. Основные положения по организации защиты информации

Понятие, цели, задачи системы защиты информации. Структура государственной системы защиты информации, задачи органов законодательной, исполнительной и судебной власти по созданию условий по защите информации.

Виды разведок: агентурная, бизнес-разведка, техническая, компьютерная разведки. Методы и способы добывания информации.

Каналы утечки, пути проникновения (нарушения) к защищаемой информации. Модель поведения нарушителя. Классификация нарушителей по возможности доступа к объекту защиты, степени подготовки и оснащенности средствами взлома, (обхода) средств защиты информации. Возможные причины, условия и обстоятельства, создающие предпосылки для свершения преступлений (правонарушений).

Тема 8 Порядок построение системы защиты информации

Комплексный и системный подход к построению системы защиты информации: понятия, цели и задачи. Исходные данные для построения системы защиты информации. Этапы и перечень работ по созданию системы защиты информации. Методика моделирования вербального объекта защиты.

Раздел 4. Контроль и ответственность, по обеспечению информационной безопасности и защиты информации

Тема 9. Контроль состояния режима безопасности и защиты информации

Основные положения по осуществлению контроля. Цели, задачи, принципы контроля. Основные мероприятия по осуществлению контроля. Проверка (контроль) выполнение требований нормативных документов по обеспечению безопасности и защиты информации, наличия конфиденциальных документов и иных носителей конфиденциальных сведений.

Тема 10. Ответственность за правонарушения и преступления в области информационной безопасности и защиты информации

Понятие и виды юридической ответственности за нарушение правовых норм по защите информации. Меры дисциплинарной ответственности согласно Трудового кодекса РФ. Административная ответственность за правонарушения в области защиты информации. Уголовная ответственность за правонарушения и преступления в области конфиденциальной информации и государственной тайны.

4. Образовательные технологии

№ п/п	Наименование раздела	Виды учебной работы	Образовательные технологии
1.	Раздел 1. Методологические аспекты информационной безопасности (ИБ) и защиты информации (ЗИ). Тема 1. Введение в дисциплину.	<i>Лекция 1. Введение в дисциплину, термины и определения, понятие и сущность ИБ.</i> <i>Содержание занятия:</i> 1. Определение основных понятий и терминов дисциплины. 2. Цели, задачи и принципы ИБ и ЗИ. <i>Самостоятельная работа:</i> 1. Связь ИБ с информатизацией общества. 2. Необходимость и значение нормативно-правового определения основных понятий.	<i>Вводная лекция с использованием видеоматериалов.</i> <i>Изучение материала по теме.</i> <i>Консультация с использованием электронной почты (ЭП).</i>
2.	Раздел 1. Методологические аспекты информационной безопасности (ИБ) и защиты информации (ЗИ) Тема 2. Базовые угрозы информационной безопасности.	<i>Лекция 2. Базовые угрозы информационной безопасности.</i> <i>Содержание занятия:</i> 1. Базовые объекты и субъекты защиты информации. 2. Источники угроз и угрозы ИБ. <i>Самостоятельная работа:</i> 1. Какие объекты защиты в информационных системах (ИС). 2. Основные источники угроз для ИС. 3. Характерные угрозы для информационных ресурсов (ИР).	<i>Лекция-визуализация с применением проектора.</i> <i>Изучение материала по теме</i> <i>Консультация с использованием электронной почты.</i>

3.	<p>Раздел 2. Информационная безопасность. Меры обеспечения информационной безопасности</p> <p>Тема 3. Законодательный, уровень обеспечения информационной безопасности</p>	<p><i>Лекция 3. Стандарты и спецификации в области ИБ.</i></p> <p><i>Содержание занятия:</i></p> <ol style="list-style-type: none"> 1. Значение стандартов в использовании информационных технологий. 2. Структура и основные положения международных актов в сфере ИБ. <p><i>Самостоятельная работа:</i></p> <ol style="list-style-type: none"> 1. Понятие и назначение стандартов. 2. Виды стандартов и критерии оценки состояния информационной безопасности. 	<p><i>Лекция-визуализация с применением проектора</i></p> <p><i>Изучение материала по теме.</i></p> <p><i>Консультация с использованием электронной почты.</i></p>
4.		<p><i>Лекция 4. Стандарты РФ в области ИБ, руководящие документы ФСТЭК РФ.</i></p> <p><i>Содержание занятия:</i></p> <ol style="list-style-type: none"> 1. Российские нормативно-правовые акты в области ИБ. 2. Базовые принципы защиты информации от несанкционированного доступа (НСД) в соответствии с нормативно-правовыми документами. <p><i>Самостоятельная работа:</i></p> <ol style="list-style-type: none"> 1. Основные федеральные органы РФ, генерирующие нормативно-правовые акты в сфере ИБ. 2. Категории ценности информации в государственных учреждениях России. 	<p><i>Лекция-визуализация с применением проектора.</i></p> <p><i>Изучение материала по тем.</i></p> <p><i>Консультация с использованием электронной почты.</i></p>
5.	<p>Раздел 2. Информационная безопасность. Меры обеспечения информационной безопасности</p> <p>Тема 4. Административный уровень, цели, задачи, управление рисками.</p>	<p><i>Лекция 5. Административный уровень: цели, задачи ИБ, управление рисками.</i></p> <p><i>Содержание занятия:</i></p> <ol style="list-style-type: none"> 1. Концепция ИБ. 2. Политика ИБ. 3. Анализ рисков ИБ. <p><i>Самостоятельная работа:</i></p> <ol style="list-style-type: none"> 1. Основные разделы политики ИБ. 2. Базовые инструментальные средства для анализа рисков. 3. Стратегии управления рисками. 	<p><i>Лекция-визуализация с применением проектора.</i></p> <p><i>Изучение материала по теме.</i></p> <p><i>Консультация с использованием электронной почты.</i></p>
6	<p>Раздел 2. Информационная безопасность. Меры обеспечения информационной безопасности.</p> <p>Тема 5.</p>	<p><i>Лекция 6. Процедурный уровень: назначение, основные направления организации работ, цели, задачи, принципы построения.</i></p> <p><i>Содержание занятия:</i></p> <ol style="list-style-type: none"> 1. Основные классы мер процедурного уровня. 2. Управление персоналом. 3. Физическая защита. 4. Поддержание работоспособности. 5. Реагирование на нарушения режима 	<p><i>Лекция-визуализация с применением проектора.</i></p> <p><i>Изучение материала по теме.</i></p>

	Процедурный уровень, назначение, основные направления организации работ, цели, задачи, принципы построения.	<p>безопасности.</p> <p>6. Планирование восстановительных работ.</p> <p><i>Коллоквиум по лабораторной работе №2.</i></p> <p><i>Самостоятельная работа:</i></p> <p>1. Минимизация привилегий и распределение обязанностей между персоналом, как основной принцип исключения от случайных ошибок и реализации преднамеренных угроз</p> <p>2. Основные требования к персоналу по поддержанию работоспособности. ИС.</p> <p>3. Основные правила по исключении дестабилизирующих факторов нарушения состояния ИБ.</p> <p>4. Действия персонала по минимизации ущерба при планировании восстановительных работ.</p>	<p>Консультация с использованием электронной почты..</p>
7	<p>Раздел 2.</p> <p>Информационная безопасность. Меры обеспечения информационной безопасности</p> <p>Тема 6.</p> <p>Программно-технический уровень обеспечения информационной информации</p>	<p><i>Лекция 7. Технология обеспечения ИБ, цели и принципы построения архитектуры ИБ.</i></p> <p><i>Содержание занятия:</i></p> <p>1. Основные понятия программно-технического уровня обеспечения ИБ.</p> <p>2. Особенности современных информационных систем, с точки зрения обеспечения ИБ.</p> <p>3. Архитектурная безопасность.</p> <p><i>Коллоквиум по лабораторной работе №12.</i></p> <p><i>Лабораторная работа 1.</i></p> <p><i>Разработка клиент-серверного приложения в Delphi.</i></p> <p><i>Самостоятельная работа:</i></p> <p>1. Основные проблемы в построении СЗИ, связанных с развитием информационных технологий.</p> <p>2. Перечислите принципы архитектурной безопасности для обеспечения конфиденциальности ИР.</p> <p>3. Перечислите принципы архитектурной безопасности для обеспечения высокой доступности (непрерывности функционирования) к ИС.</p>	<p><i>Лекция-визуализация с применением проектора.</i></p> <p><i>Изучение материала по теме.</i></p> <p><i>Занятия с использованием специализированного ПО.</i></p> <p><i>Консультация с использованием электронной почты.</i></p>
8		<p><i>Лекция 8. Сервисы ИБ: назначение, функции, методы реализации сервисов ИБ.</i></p> <p><i>Содержание занятия:</i></p> <p>1. Идентификация и аутентификация пользователей.</p> <p>2. Управление доступом к информации.</p> <p>3. Протоколирование и аудит ИБ.</p> <p>4. Базовые методы криптографического преобразования данных.</p> <p>5. Экранирование как защита информации в сетях.</p>	<p><i>Лекция-визуализация с применением проектора.</i></p> <p><i>Изучение материала по теме.</i></p>

		<p>Коллоквиум по лабораторной работе №4.</p> <p>Самостоятельная работа:</p> <ol style="list-style-type: none"> 1. Основные группы методов аутентификации. 1. Особенности протоколирования аудита. 2. Основные группы классов защищенности ИС. 2. Симметричные и ассиметричные криптосистемы. 3. Компьютерная стеганография. 4. Основные классы межсетевых экранов. 	<p>Занятия с использованием специализированного ПО.</p> <p>Проверка домашнего задания.</p> <p>Консультация с использованием электронной почты.</p>
8	<p>Раздел 3. Система защиты информации</p> <p>Тема 7.</p> <p>Основные положения по организации защиты информации</p>	<p>Лекция 9 Развитие системы защиты информации.</p> <p>Содержание занятия:</p> <ol style="list-style-type: none"> 1. Этапы развития системы защиты информации в настоящее время 2. Государственная система обеспечения информационной безопасности (ГСЗИ) 3. Классификация нарушителя. 4. Этапы реализация угроз безопасности информации нарушителем. 5. Каналы утечки, пути несанкционированного доступа к защищаемой информации. <p>Самостоятельная работа:</p> <ol style="list-style-type: none"> 1. Структура государственной системы защиты информации, задачи органов законодательной, исполнительной и судебной власти по созданию условий по обеспечению информационной безопасности. 2. Классификация нарушителей по возможности доступа к объекту защиты, степени подготовки и оснащенности средствами взлома, обхода средств защиты информации. 3. Возможные причины, условия и обстоятельства, создающие предпосылки для свершения преступлений (правонарушений). 	<p>Лекция-визуализация с применением проектора.</p> <p>Изучение материала по теме.</p> <p>Консультация с использованием электронной почты.</p>
8	<p>Раздел 3. Система защиты информации</p> <p>Тема 8.</p> <p>Порядок построение системы защиты информации</p>	<p>Лекция 10. Построение системы защиты информации.</p> <p>Содержание занятия:</p> <ol style="list-style-type: none"> 1. Комплексный подход к построению системы защиты информации. 2. Системный подход к построению системы защиты информации. 3. Порядок построения системы защиты информации. 4. Методы оценки защищенности системы защиты информации на предприятии. <p>Лабораторная работа №2.</p> <p>Решение в локальной сети задачи аутентификация пользователей.</p> <p>Самостоятельная работа:</p> <ol style="list-style-type: none"> 1. Что понимается под комплексным подходом 	<p>Лекция-визуализация с применением проектора.</p> <p>Изучение материала по теме.</p> <p>Занятия с использованием специализированного ПО.</p> <p>Консультация с использованием</p>

		<p>к защите информации.</p> <p>2. Что понимается под системным подходом к защите информации.</p> <p>3. Какие исходные данные для построения системы защиты информации.</p> <p>4. Структура системы защиты информации на предприятиях.</p> <p>5. Перечислите этапы и перечень работ по созданию системы защиты информации.</p>	<i>электронной почты.</i>
8	<p>Раздел 4. Контроль и ответственность по обеспечению информационной безопасности и защиты информации</p> <p>Тема 9. Контроль состояния режима безопасности и защиты информации</p>	<p><i>Лекция 11. Контроль по обеспечению информационно безопасности и защиты информации.</i></p> <p><i>Содержание занятия:</i></p> <p>1. Цели, задачи и принципы контроля.</p> <p>2. Основные мероприятия по осуществлению контроля.</p> <p>3. Проверка (контроль) режима конфиденциальности, наличия конфиденциальных документов и иных носителей конфиденциальной информации.</p> <p>Самостоятельная работа:</p> <p>1. Основные положения по осуществлению контроля. Цели, задачи, принципы контроля.</p> <p>2. Основные мероприятия по осуществлению контроля.</p> <p>3. Проверка (контроль) наличия конфиденциальных документов и иных носителей конфиденциальных сведений.</p> <p>4. Проведение служебного расследования по фактам нарушения требований режима конфиденциальности..</p>	<p><i>Лекция-визуализация с применением проектора.</i></p> <p><i>Изучение материала по теме.</i></p> <p><i>Консультация с использованием электронной почты.</i></p>
8	<p>Раздел 4. Контроль и ответственность по обеспечению информационной безопасности и защиты информации</p> <p>Тема 10. Ответственность за правонарушения и преступления в области информационной безопасности и защиты информации</p>	<p><i>Лекция 12. Ответственность за правонарушения и преступления в области информационной безопасности и защиты информации.</i></p> <p><i>Содержание занятия:</i></p> <p>1. Понятие и виды юридической ответственности за нарушение правовых норм.</p> <p>2. Меры дисциплинарной ответственности согласно Трудового кодекса РФ.</p> <p>3. Административная ответственность за правонарушения в области конфиденциальной информации.</p> <p>4. Уголовная ответственность за правонарушения и преступления в области конфиденциальной информации.</p> <p>5. Уголовная ответственность за правонарушения и преступления в области защиты государственной тайны.</p> <p>Самостоятельная работа:</p> <p>1. Понятие и виды юридической ответственности за нарушение правовых норм по защите информации.</p>	<p><i>Лекция-визуализация с применением проектора.</i></p> <p><i>Изучение материала по теме.</i></p> <p><i>Консультация с использованием электронной почты.</i></p>

		2. Меры дисциплинарной ответственности согласно Трудового кодекса РФ. 3. Административная ответственность за правонарушения в области защиты информации. 4. Уголовная ответственность за правонарушения и преступления в области конфиденциальной информации. 5. Уголовная ответственность за правонарушения и преступления в области государственной тайны.	
--	--	---	--

5. Оценка планируемых результатов обучения

5.1. Система оценивания

Форма контроля	Макс. количество баллов	
	За одну работу	Всего
Текущий контроль:		
- <i>опрос</i> ;	5 баллов	30 баллов
- <i>защита лабораторных работ</i> ;	5 баллов	20 баллов
- <i>тестирование</i> ;	10 баллов	10 баллов
Промежуточная аттестация (<i>зачет</i>);		40 баллов
Итого за семестр (дисциплину).		100 баллов

Текущий контроль

При оценивании устного опроса и участия в дискуссии на семинаре учитываются:

- степень раскрытия содержания материала (0-2 балла);
- изложение материала (грамотность речи, точность использования терминологии и символики, логическая последовательность изложения материала (0-2 балла);
- знание теории изученных вопросов, сформированность и устойчивость используемых при ответе умений и навыков (0-1 балл).

При оценивании защиты лабораторной работы учитываются:

- полнота выполненной работы (задание выполнено не полностью и/или допущены две и более ошибки или три и более неточности) – 1-4 балла;
- обоснованность содержания и выводов работы (задание выполнено полностью, но обоснование содержания и выводов недостаточны, но рассуждения верны) – 5-8 баллов;
- работа выполнена полностью, в рассуждениях и обосновании нет пробелов или ошибок, возможна одна неточность -9-10 баллов.

При оценивании контрольной, практической работы учитываются:

- полнота выполненной работы (задание выполнено не полностью и/или допущены две и более ошибки или три и более неточности) – 1-4 балла;
- обоснованность содержания и выводов работы (задание выполнено полностью, но обоснование содержания и выводов недостаточны, но рассуждения верны) – 5-8 баллов;
- работа выполнена полностью, в рассуждениях и обосновании нет пробелов или ошибок, возможна одна неточность -9-10 баллов.

Критерии оценивания при тестировании.

При тестировании студент должен ответить на 20 вопросов.

При оценивании ответа на вопрос учитывается:

- ответ содержит менее 20% правильного ответа (1-4 балла);
- ответ содержит 21-50 % правильного ответа (5-9 баллов);
- ответ содержит 51-80 % правильного ответа (10-14 баллов);
- ответ содержит 90% и более правильного ответа (15-20 баллов).

Критерии оценивания при сдаче зачетов.

При сдаче зачета студент должен ответить на 3 вопроса (два вопроса теоретического характера и один вопрос практического характера).

При оценивании ответа на вопрос теоретического характера учитывается:

- теоретическое содержание не освоено, знание материала носит фрагментарный характер, наличие грубых ошибок в ответе (1-3 балла);
- теоретическое содержание освоено частично, допущено не более двух-трех недочетов (4-7 баллов);
- теоретическое содержание освоено почти полностью, допущено не более одного-двух недочетов, но обучающийся смог бы их исправить самостоятельно (8-11 баллов);
- теоретическое содержание освоено полностью, ответ построен по собственному плану (12-15 баллов).

При оценивании ответа на вопрос практического характера учитывается:

- ответ содержит менее 20% правильного решения (1-2 балла);
- ответ содержит 21-89 % правильного решения (3-8 баллов);
- ответ содержит 90% и более правильного решения (9-10 баллов).

Полученный совокупный результат конвертируется в традиционную шкалу оценок и в шкалу оценок Европейской системы переноса и накопления кредитов (European Credit Transfer System; далее – ECTS) в соответствии с таблицей:

100-балльная шкала	Традиционная шкала		Шкала ECTS
95 – 100	отлично		A
83 – 94		зачтено	B

68 – 82	хорошо		C
56 – 67	удовлетворительно		D
50 – 55			E
20 – 49	неудовлетворительно	не зачтено	FX
0 – 19			F

5.2.Критерии выставления оценок

Баллы/ Шкала ECTS	Оценка по дисциплине	Критерии оценки результатов обучения по дисциплине
100-83/ A,B	«отлично»/ «зачтено (отлично)»/ «зачтено»	<p>Выставляется обучающемуся, если он глубоко и прочно усвоил теоретический и практический материал, может продемонстрировать это на занятиях и в ходе промежуточной аттестации.</p> <p>Обучающийся исчерпывающе и логически стройно излагает учебный материал, умеет увязывать теорию с практикой, справляется с решением задач профессиональной направленности высокого уровня сложности, правильно обосновывает принятые решения.</p> <p>Свободно ориентируется в учебной и профессиональной литературе.</p> <p>Оценка по дисциплине выставляется обучающемуся с учётом результатов текущей и промежуточной аттестации.</p> <p>Компетенции, закреплённые за дисциплиной, сформированы на уровне – «высокий».</p>
82-68/ C	«хорошо»/ «зачтено (хорошо)»/ «зачтено»	<p>Выставляется обучающемуся, если он знает теоретический и практический материал, грамотно и по существу излагает его на занятиях и в ходе промежуточной аттестации, не допуская существенных неточностей.</p> <p>Обучающийся правильно применяет теоретические положения при решении практических задач профессиональной направленности разного уровня сложности, владеет необходимыми для этого навыками и приёмами.</p> <p>Достаточно хорошо ориентируется в учебной и профессиональной литературе.</p> <p>Оценка по дисциплине выставляется обучающемуся с учётом результатов текущей и промежуточной аттестации.</p> <p>Компетенции, закреплённые за дисциплиной, сформированы на уровне – «хороший».</p>
67-50/ D,E	«удовлетворительно»/ «зачтено (удовлетворительно)»/ «зачтено»	<p>Выставляется обучающемуся, если он знает на базовом уровне теоретический и практический материал, допускает отдельные ошибки при его изложении на занятиях и в ходе промежуточной аттестации.</p> <p>Обучающийся испытывает определённые затруднения в применении теоретических положений при решении практических задач профессиональной направленности стандартного уровня сложности, владеет необходимыми</p>

Баллы/ Шкала ECTS	Оценка по дисциплине	Критерии оценки результатов обучения по дисциплине
		ми для этого базовыми навыками и приёмами. Демонстрирует достаточный уровень знания учебной литературы по дисциплине. Оценка по дисциплине выставляются обучающемуся с учётом результатов текущей и промежуточной аттестации. Компетенции, закреплённые за дисциплиной, сформированы на уровне – «достаточный».
49-0/ F,FX	«неудовлетворительно»/ не зачтено	Выставляется обучающемуся, если он не знает на базовом уровне теоретический и практический материал, допускает грубые ошибки при его изложении на занятиях и в ходе промежуточной аттестации. Обучающийся испытывает серьёзные затруднения в применении теоретических положений при решении практических задач профессиональной направленности стандартного уровня сложности, не владеет необходимыми для этого навыками и приёмами. Демонстрирует фрагментарные знания учебной литературы по дисциплине. Оценка по дисциплине выставляются обучающемуся с учётом результатов текущей и промежуточной аттестации. Компетенции на уровне «достаточный», закреплённые за дисциплиной, не сформированы.

5.3. Оценочные средства (материалы) для текущего контроля успеваемости, промежуточной аттестации обучающихся по дисциплине

Текущий контроль

Устный опрос

Устный опрос – это средство контроля, организованное как специальная беседа преподавателя с обучающимся на темы, связанные с изучаемой дисциплиной, и рассчитанное на выяснение объема знаний обучающегося по определенному разделу, теме, проблеме и т.п.

Перечень устных вопросов для проверки знаний

1. Концепция объектно-ориентированного подхода к обеспечению ИБ.
2. Основные составляющие информационной безопасности (ИБ).
3. Недостатки традиционного подхода к обеспечению ИБ.
4. Характеристика наиболее распространенных угроз.
5. Критерии классификации угроз.
6. Примеры угроз доступности.
7. Основные угрозы целостности

8. Основные угрозы конфиденциальности.
9. Что такое законодательный уровень ИБ и почему он важен?
10. Основные законы РФ в области ИБ.
11. Основные зарубежные стандарты в области ИБ.
12. Что такое оценочные стандарты и технические спецификации?
13. Рекомендации X.800.
14. Стандарт ISO/ IEC.
15. Что такое политика безопасности и ее актуальность?
16. Что такое программа безопасности и ее актуальность?
17. Этапы управления рисками в системе защиты информации.
18. Основные программно-технические меры защиты.
19. Технология идентификации и аутентификации.
20. Технология управления доступом.
21. Протоколирование и аудит.
22. Технология шифрования.
23. Архитектурные аспекты экранирования.
24. Классификация межсетевых экранов.
25. Вредоносное программное обеспечение.
26. Анализ защищенности.
27. Возможности типичные схем туннелирования.
28. Задачи органов законодательной, исполнительной и судебной власти по созданию условий по обеспечению информационной безопасности.
29. Классификация нарушителей по возможности доступа к объекту защиты,
- 30. Возможные причины, условия и обстоятельства, создающие предпосылки для совершения преступлений (правонарушений).**
31. Каналы утечки информации, пути несанкционированного доступа (проникновения) нарушения.
32. Что понимается под комплексным подходом к защите информации.
33. Что понимается под системным подходом к защите информации.
34. Какие исходные данные необходимы для построения системы защиты информации.
35. Перечислите этапы и перечень работ по созданию системы защиты информации.
36. Порядок разработки вербального объекта защиты
37. Основные положения по осуществлению контроля. Цели, задачи, принципы контроля.
38. Основные мероприятия по осуществлению контроля.

39. Проверка (контроль) наличия конфиденциальных документов и иных носителей конфиденциальных сведений.
40. Проведение служебного расследования по фактам нарушения требований режима конфиденциальности.
41. Понятие и виды юридической ответственности за нарушение правовых норм по защите информации.
42. Меры дисциплинарной ответственности согласно Трудового кодекса РФ.
43. Административная ответственность за правонарушения в области защиты информации.
44. Уголовная ответственность за правонарушения и преступления в области конфиденциальной информации.
45. Уголовная ответственность за правонарушения и преступления в области государственной тайны.

Контрольное тестирование (текущий контроль)

Примерные тестовые задания:

1. В соответствии с действующим законом РФ понятие «информация», которая подлежит защите, определяется как:

- 1) сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления;
- 2) сведения (сообщения, данные) независимо от формы их представления;
- 3) сведения, рассматриваемые в процессе их передачи или восприятия, позволяющие расширить знания об интересующем объекте;
- 4) сведения, передаваемые одними людьми другим людям устным, письменным или каким-либо другим способом.

2. Конфиденциальность информации:

- 1) сведения, в установленном порядке отнесенные руководителем к информации ограниченного доступа;
- 2) документированная информация, доступ к которой ограничивается в соответствии с законодательством РФ;
- 3) отдельные закрытые документы (массивы документов в закрытых информационных системах);
- 4) зафиксированная на материальном носителе информация с реквизитами, позволяющими ее идентифицировать.

3. В соответствии с действующим законом РФ информационная безопасность определяется как:

1) процесс организации защищённости информационной среды от воздействия источников угроз, обеспечивающее её формирование, использование, развитие в интересах граждан, общества, государства;

2) *состояние защищённости информационной среды от воздействия источников угроз, обеспечивающее её формирование, использование, развитие в интересах граждан, общества, государства;*

3) состояние защищённости информационных ресурсов от воздействия источников угроз, обеспечивающее её формирование, использование, развитие в интересах граждан, общества, государства;

4) состояние защищённости информационных систем от воздействия источников угроз, обеспечивающее её формирование, использование, развитие в интересах граждан, общества, государства.

4. Защита информации от несанкционированного доступа:

1) защита информации, направленная на предотвращение получения защищаемой информации заинтересованными субъектами с нарушением требований нормативных и правовых документов;

2) защита информации, направленная на предотвращение получения защищаемой информации заинтересованными субъектами с нарушением прав обладателями информации;

3) *защита информации, направленная на предотвращение получения защищаемой информации заинтересованными субъектами с нарушением установленных нормативными и правовыми документами (актами) или обладателями информации прав или правил разграничения доступа к защищаемой информации;*

4) предотвращение получения защищаемой информации с нарушением установленных требований к защищаемой информации.

5. Источник угрозы безопасности информации:

1) субъект (физическое лицо), являющийся непосредственной причиной возникновения угрозы безопасности информации;

2) субъект (физическое лицо, материальный объект), меняющий состояние информационной безопасности;

3) *субъект (физическое лицо, материальный объект или физическое явление), являющийся непосредственной причиной возникновения угрозы безопасности информации;*

4) субъект (физическое лицо, материальный объект или физическое явление), создающих потенциальную или реально существующую опасность нарушения безопасности информации.

6. Угроза безопасности информации:

- 1) совокупность условий и факторов, создающих потенциальную опасность нарушения безопасности информации;
- 2) совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации;
- 3) субъект (физическое лицо, материальный объект), являющийся непосредственной причиной возникновения угрозы безопасности информации;
- 4) субъект (физическое лицо, материальный объект), являющийся причиной изменения состояния безопасности информации.

7. К основным методам реализации НСД к информации не относится:

- 1) «маскарад»;
- 2) «подкладывание свиньи»;
- 3) «карнавал»;
- 4) «атака»;

8. Борьбу с компьютерными преступлениями в России не ведут:

- 1) структуры ФСБ;
- 2) отделы департамента «С» МЧС России;
- 3) отделы «К» МВД России;
- 4) спецподразделения Управления по борьбе с экономическими преступлениями МВД России.

9. Какой из видов компьютерных преступлений наиболее распространен в настоящее время?

- 1) кража средств компьютерной техники;
- 2) несанкционированный доступ к информации;
- 3) изготовление или распространение вредоносных программ;
- 4) перехват информации.

10. К основным свойствам информации, подлежащим защите, не относится:

- 1) доступность;
- 2) конфиденциальность;
- 3) достоверность;
- 4) целостность.

11. В соответствии с действующим законом «конфиденциальность информации» определяется как:

- 1) свойство информации, позволяющее ее обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду;

2) *обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя;*

3) *свойство информации, доступ к которой ограничивается в соответствии с законодательством РФ;*

4) *обязательное для соблюдения физическим или юридическим лицом требование не допускать распространение информации без согласия её обладателя.*

12. При реализации мандатной политики доступа не реализуется следующий критерий:

1) *все субъекты и объекты системы должны быть идентифицированы;*

2) *права доступа субъекта к объекту системы определяются на основании некоторого правила;*

3) *каждому объекту системы присваивается метка критичности;*

4) *каждому субъекту системы присвоен уровень прозрачности, определяющий максимальное значение метки критичности объектов, к которым субъект имеет доступ.*

13. Что не представлено в матрице доступа к информации:

1) *субъект доступа;*

2) *вид доступа;*

3) *правило доступа;*

4) *объект доступа.*

14. Новое семейство международных стандартов на системы управления информационной безопасностью имеет код:

1) *17000;*

2) *27000;*

3) *37000;*

4) *47000.*

15. В криптосистемах используется в основном следующий тип шифрования:

1) *блочный;*

2) *поточковый;*

3) *символьный;*

4) *смешанный.*

16. Какое из ниже перечисленных направлений не входит в состав физической защиты:

1) *физическое управление доступом;*

2) *разделение доступа пользователей;*

3) *защита от перехвата данных;*

4) *защита поддерживающей инфраструктуры.*

17. Гаммирование – это:

- 1) один из функциональных методов аутентификации;
- 2) разновидность стеганографического метода защиты информации;
- 3) способ шифрования информации;
- 4) метод подготовки сообщения для преодоления межсетевого экрана.

18. Что является объектом защиты в области информационной безопасности и защиты информации:

- 1) информация;
- 2) носители информации;
- 3) информационные процессы;
- 4) информация, носители информации, информационные процессы.

19. Какого средства для защиты информации или её уничтожения не существует:

- 1) «информационный сейф»;
- 2) «цунами»;
- 3) «торнадо»;
- 4) «тень».

20. Программные вирусы не классифицируются по следующему признаку:

- 1) по среде обитания вируса;
- 2) по способу заражения;
- 3) по деструктивным возможностям;
- 4) по способу размножения.

21. Преимуществом мандатного метода управления доступом не является:

- 1) обеспечение более высокой надежности работы самой ИС;
- 2) простота определения правил разграничения доступа;
- 3) широкое распространение данного метода для работы с конфиденциальной информацией;
- 4) предотвращение утечки информации из объектов с высокой меткой конфиденциальности в объекты с низкой меткой конфиденциальности.

22. Современная криптография не включает следующий раздел:

- 1) симметричные криптосистемы;
- 2) криптосистемы с открытым ключом;
- 3) системы формирования хэш-функций;
- 4) управление ключами.

23. Симметричные криптосистемы не используют следующий алгоритм шифрования:

- 1) DES;

- 2) IDEA;
- 3) ГОСТ 28147-89;
- 4) алгоритм Диффи-Хеллмана;

24. Укажите, какой из указанных методов закрытия информации наиболее трудоёмок:

- 1) перестановка;
- 2) аналитические преобразования;
- 3) гаммирование;
- 4) замена.

25. В число основных принципов, необходимых для достижения архитектурной безопасности защищаемых систем, не входит следующий:

- 1) невозможность миновать защитные средства;
- 2) ликвидация самого слабого звена;
- 3) невозможность перехода системы в небезопасное состояние;
- 4) эшелонированность обороны.

26. Какой из указанных функций не является сервисом для аппаратно-программных средств защиты информации:

- 1) идентификация и аутентификация;
- 2) криптографическая защита;
- 3) управление персоналом;
- 4) экранирование.

27. Количество классов защищенности для межсетевых экранов:

- 1) три;
- 2) четыре;
- 3) пять;

28. К основным мерам по защите криптографических ключей не относится следующая:

- 1) ограничение круга лиц, допущенных к работе с ключами;
- 2) регламентация рассылки, хранения и уничтожения ключей;
- 3) регламентация порядка смены ключей;
- 4) применение метода конгруэнтных сечений для хранения ключей.

29. В настоящее время брандмауэр - это:

- 1) специализированный программный комплекс;
- 2) специальное техническое средство;
- 3) специализированный программно-аппаратный комплекс;
- 4) разновидность криптографического средства защиты информации.

30. Цель защиты информации:

- 1) заранее намеченный результат защиты информации по предотвращению ущерба обладателю информации;
- 2) *заранее намеченный результат защиты информации по предотвращению ущерба обладателю информации из-за возможной утечки информации и (или) несанкционированного и непреднамеренного воздействия на информацию;*
- 3) исключение (недопущения) реализации угроз безопасности информации;
- 4) защита информации от её утечки.

31. Эффективность защиты информации:

- 1) выполнение требований нормативных документов по защите информации;
 - 2) выполнение рекомендаций руководящих документов по защите информации;
 - 3) степень соответствия результатов защиты информации требованиям по защите информации;
 - 4) *степень соответствия результатов защиты информации цели защиты информации.*
- рабочего дня.

32. Минимизация привилегий для работника:

- 1) минимизация полномочий по исполнению своих служебных обязанностей;
- 2) *выделять пользователям только те права доступа, которые необходимы им для выполнения служебных обязанностей;*
- 3) так распределять роли и ответственность, чтобы один человек не мог нарушить критически важный для организации процесс;
- 4) минимизация поставленных задач для достижения поставленных целей.

33. Разделение обязанностей для работника:

- 1) минимизация полномочий по исполнению своих служебных обязанностей;
- 2) выделять пользователям только те права доступа, которые необходимы им для выполнения служебных обязанностей;
- 3) *так распределять роли и ответственность, чтобы один человек не мог нарушить критически важный для организации процесс;*
- 4) минимизация полномочий по исполнению своих служебных обязанностей.

34. Основной целью контроля (проверки) состояния защиты конфиденциальной информации на предприятии является:

- 1) установление правил по защите сведений ограниченного доступа;
- 2) *проверка наличия носителей сведений конфиденциального характера и соблюдения установленного порядка обращения с ними;*
- 3) проверка соблюдения требований по порядку засекречивания сведений и присвоению грифа секретности носителям;

4) проверка правильности учета, хранения, размножения, уничтожения носителей сведений.

35. Контроль эффективности защиты информации:

1) проверка соответствия качественных показателей эффективности мероприятий по защите информации требованиям или нормам эффективности защиты информации;

2) *проверка соответствия качественных и количественных показателей эффективности мероприятий по защите информации требованиям или нормам эффективности защиты информации;*

3) проверка соответствия эффективности мероприятий по защите информации на объекте защиты требованиям или нормам эффективности защиты информации;

4) проверка соответствия выполнения на объекте защиты требований по защите информации.

36. В соответствии с УК РФ неправомерный доступ к компьютерной информации:

1) ст.271;

2) *ст.272;*

3) ст.273;

4) ст.274;

Контрольные вопросы для сдачи зачета (промежуточная аттестация)

1. Основные понятия информации, источники информации, свойства информации.
2. Классификация информации в правовой системе от порядка ее предоставления или распространения.
3. Понятие информационной безопасности, цели, задачи, принципы обеспечения безопасности информации.
4. Важность и сложность проблемы информационной безопасности.
5. Потенциальные источники угроз и способы нарушения информационной безопасности.
6. Определение и критерии классификации угроз безопасности информации.
7. Наиболее распространенные угрозы доступности.
8. Основные угрозы целостности.
9. Основные угрозы конфиденциальности.
10. Нормативное правовое обеспечение информационной безопасности Российской Федерации.
11. Стандарты и спецификации в области информационной безопасности.
12. Стандарты и спецификации в области информационной безопасности, руководящие документы ФСТЭК (Гостехкомиссии) России.
13. Административный уровень информационной безопасности: основные понятия, цели и задачи, политика безопасности.

14. Административный уровень информационной безопасности, политика информационной безопасности.

15. Административный уровень информационной безопасности, программа информационной безопасности.

16. Управления рисками: понятия по анализу рисков, основные этапы управления рисками.

17. Процедурный уровень информационной безопасности: основные классы мер процедурного уровня.

18. Процедурный уровень информационной безопасности: управление персоналом.

19. Процедурный уровень информационной безопасности: физическая защита, поддержание работоспособности.

20. Процедурный уровень информационной безопасности: реагирование на нарушения режима безопасности, планирование восстановительных работ.

21. Основные понятия программно-технического уровня информационной безопасности.

22. Принципы построения архитектурной безопасности информационных систем.

23. Идентификация и аутентификация: основные понятия.

24. Идентификация и аутентификация: парольная аутентификация, одноразовые пароли.

25. Идентификация и аутентификация: сервер аутентификации Kerberos.

26. Идентификация/аутентификация с помощью биометрических данных.

27. Управление доступом: основные понятия, ролевое управление доступом.

28. Управление доступом: возможный подход к управлению доступом в распределенной объектной среде.

29. Компьютерные вирусы: определение компьютерного вируса, виды и способы размножения, степень нанесения ущерба компьютерного вируса.

30. Компьютерные вирусы: методы и средства нейтрализации программных вирусов.

31. Протоколирование и аудит: назначение, задачи, функции.

32. Шифрование информации: назначение, методы и способы шифрования информации.

33. Контроль целостности данных: назначение, задачи, функции.

34. Межсетевые экраны: архитектурные аспекты межсетевых экранов.

35. Межсетевые экраны: классификация межсетевых экранов.

36. Сервис анализа защищенности: задачи, назначение.

37. Туннелирование и управление: назначение, задачи, функциональные области управления.

38. Обеспечение высокой доступности: основные понятия, основы мер обеспечения высокой доступности.

39. Обеспечение высокой доступности: отказоустойчивость и зона риска.

40. Обеспечение высокой доступности: обеспечение отказоустойчивости информационных систем.

41. Структура государственной системы защиты информации РФ, задачи органов законодательной, исполнительной и судебной власти по созданию условий по обеспечению информационной безопасности.

42. Классификация нарушителей по возможности доступа к объекту (предмету) защиты, степени подготовки и оснащенности средствами взлома, обхода средств защиты информации.

43. Возможные причины, условия и обстоятельства, создающие предпосылки для совершения преступлений (правонарушений).

44. Каналы утечки информации, пути несанкционированного доступа (проникновения) нарушения к объекту защиты.

45. Методы способы несанкционированного доступа (НСД) к информации при ее обработке на СВТ (АС).

46. Комплексный подход к построению системы защиты информации.

47. Системный подход к защите информации.

48. Исходные данные для построения системы защиты информации.

49. Типовая структура системы защиты информации на предприятиях.

50. Цели и задачи системы управления и организации работ по обеспечению безопасности информации на предприятии.

51. Основные положения по осуществлению контроля.

52. Основные мероприятия по осуществлению контроля.

53. Проверка (контроль) наличия конфиденциальных документов и иных носителей конфиденциальных сведений.

54. Проведение служебного расследования по фактам нарушения требований режима конфиденциальности.

55. Понятие и виды юридической ответственности за нарушение правовых норм по защите информации.

56. Меры дисциплинарной ответственности согласно Трудового кодекса РФ.

57. Административная ответственность за правонарушения в области защиты интеллектуальной собственности и информационной безопасности.

58. Уголовная ответственность за правонарушения в области конфиденциальной информации.

6. Учебно-методическое и информационное обеспечение дисциплины

6.1.Список источников и литературы

1. Доктрина информационной безопасности РФ. Утверждена Президентом Российской Федерации от 05.12.2016г. №646.
2. Федеральный закон РФ Об информации, информационных технологиях и о защите информации» от 27 июля 2006 № 149-ФЗ.
3. ГОСТ Р 50922-2006. Защита информации. Основные термины и определения
4. ГОСТ Р 51275-2006 Защита информации. Объект информации. Общие положения
5. ГОСТ Р ИСО/МЭК 17799-2005 Практические правила управления информационной безопасностью
6. ГОСТ Р ИСО/МЭК 15408-1 (15408-2, 15408-3) Критерии оценки безопасности информационных технологий
7. РД. Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации, Решение Председателя Гостехкомиссии России от 30.03.1992
8. РД. АС. Защита от НСД к информации. Классификация АС и требования по защите информации. Решение Председателя Гостехкомиссии России от 30. 03.1992

Рекомендуемая литература (основная)

9. В.А. Ворона. В.А. Тихонов, Л.В. Митрякова, Теоретические основы обеспечение безопасности объектов информатизации, учебное пособие для вузов _М: Горячая линия – Телеком, 2016 -304с. ISBN 978-5-9912-0524-5
10. Мельников В.П., Клейменов С.А, Петраков А.М. Информационная безопасность: учебник для вузов. - [7-е изд.]. - М.: Акад. проект, 2012.
11. Арутюнов В.В., Гудов Г.Н. Информационная безопасность и защита информации. — М.: МФЮА, 2012. - 360 с.
12. Вепрев С.Б., Халяпин Д.Б., Лобашев А.К., Гудов Г.Н. «Противодействие экономическому шпионажу» Электронное учебно-методическое пособие, ООО Издательский дом «Афина» С-П 2013г.
13. Гудов Г.Н. Организация и управление службой защиты информации. Учебное пособие М.: МФЮА, 2016. - 234с.

14. Центр исследования компьютерной преступности [Электронный ресурс]. Г. Маклаков, Научно-методологические аспекты подготовки специалистов в области информационной безопасности, статья - <http://www.crime-research.ru/>
15. Обзор зарубежного законодательства в области информационной безопасности [Электронный ресурс], статья - <http://www.intuit.ru/department/security/secbasics/4/4.html>
16. Журнал «Информационное право» [Электронный ресурс]. <http://www.infolaw.ru/lib / 2005-1-internet-and-law>.
17. Интернет-технологии: Учебное пособие / С.Р. Гуриков. - М.: Форум: НИЦ ИНФРА-М, 2015. - 184 с. Режим доступа: <http://znanium.com/catalog.php?bookinfo=488074>

Печатные издания, имеющиеся в наличии в Научной библиотеке РГГУ (на всех территориях)

18. Подготовка объекта информатизации к аттестации по требованиям безопасности / Е. Г. Воробьев, С. В. Войцеховский ; под ред. Н. М. Михайлова. - 88 с. ; Ч. 2 : , [2013].
19. Лобашев А.К., Халяпин Д.Б., Гудов Г.Н. Противодействие экономическому шпионажу (Информационное пособие на CD). –СПб.: Издательский дом «Афина», 2012.
20. Комплект организационно-распорядительных документов для аттестации объектов информатизации автоматизированной информационной системы; Ч. 3: , [2013].

Рекомендуемая литература (дополнительная):

21. Башлы П. Н. Информационная безопасность и защита информации [Электронный ресурс] : Учебник / П. Н. Башлы, А. В. Бабаш, Е. К. Баранова. - М.: РИОР, 2013. - 222 с.
22. Белый А.Ф. Управление функциональной устойчивостью комплексов средств автоматизации в условиях программно-аппаратных воздействий /Стратегическая стабильность №4 (57), 2011, с.34-36.
23. Тихонов В. А., Райх В. В. Информационная безопасность. Концептуальные, правовые, организационные и технические аспекты. – М.: Гелиос АРВ, 2006.-275с

6.2. Перечень ресурсов информационно-телекоммуникационной сети «Интернет»

1. Информационный бюллетень Jet Info [Электронный ресурс]. - Электрон. дан. - [М., 2014]. - Режим доступа свобод.: <http://www.jetinfo.ru/> .
2. Официальный сайт Российской государственной библиотеки [Электронный ресурс]. - Электрон. дан. - [М., 2013]. - Режим доступа свобод.: <http://www.rsl.ru/> .
3. Официальный сайт Российской национальной библиотеки [Электронный ресурс]. - Электрон. дан. - [М., 2014]. - Режим доступа свобод.: <http://www.nlr.ru/> .
4. Glossary Commander. Служба тематических толковых словарей [Электронный ресурс]. - Электрон. дан. - [М., 2008]. - Режим доступа свобод.: <http://glossary.ru/> .
5. Сайт справочно-правовой системы по федеральному и региональным законодательст-

вам России - <http://pravo.ru/>

6. Официальный интернет-портал правовой информации - <http://pravo.gov.ru>
7. Информационный портал в области защиты информации <http://www.securitylab.ru>
8. Обзор зарубежного законодательства в области информационной безопасности [Электронный ресурс], статья - <http://www.intuit.ru/departament/security/secbasics/4/4.html>.
9. Портал ФСТЭК <http://www.fstec.ru>
10. Сайт электронной библиотеки <http://www.iprbookshop.ru>

7. Материально-техническое обеспечение дисциплины

Для проведения занятий по дисциплине необходимо:

1. Сервер – 1.
2. ПЭВМ – 25 комплектов, объединенные в локальную сеть, с установленным ПО MS WINDOWS.
3. Мультимедийный видеопроектор.
4. Экран со стойкой.

лекционных занятий - аудитория с компьютером и проектором,

лабораторных занятий – компьютерный класс с установленным ПО MS WINDOWS, CSS, объединенный локальной информационной сетью по технологии клиент-сервер, интегрированной в домен с выходом в Интернет

промежуточной аттестации (зачет с оценкой) – аудитория.

Лабораторные работы занятия проводятся в учебных группах (подгруппах) и имеют своей целью:

- 1) закрепление теоретических основ дисциплины, излагаемых в лекционном курсе, а также самостоятельно изучаемых студентами;
- 2) формирование практических навыков по использованию технических средств защиты информации;
- 3) научить студентов использовать техники экспериментальных исследований и анализа полученных результатов;
- 4) привитие навыков работы с лабораторным оборудованием, контрольно-измерительными приборами и вычислительной техникой.

К выполнению лабораторных работ допускаются обучаемые, уяснившие тему, цель, содержание работы, правила техники безопасности и эксплуатации ПЭВМ и знающие теоретический материал по теме лабораторной работы.

Для материально-технического обеспечения дисциплины «Техническая защита информации» необходимы:

При подготовке к лабораторной работе необходимо:

1. Изучить правила техники безопасности и правила технической эксплуатации ПЭВМ и программы Electronics Workbench.
2. Подготовить бланк отчета по лабораторной работе, куда занести тему, цель работы, ее содержание, состав и назначение применяемых для измерений приборов, а также таблицы наблюдений измеряемых величин.
3. Подготовиться к индивидуальному собеседованию по теме лабораторной работы.

Правила техники безопасности при работе на ПЭВМ.

Каждый обучаемый обязан знать и неукоснительно выполнять основные требования правил техники безопасности и расписаться за их изучение.

К самостоятельной работе в классе ПЭВМ допускаются лица, прошедшие инструктаж по технике безопасности.

Общие требования:

1. К работе на ПЭВМ, не связанной с их обслуживанием, допускаются лица, обученные безопасным методам работы с ПЭВМ, а также прошедшие проверку знаний и периодический инструктаж.
2. ПЭВМ должны удовлетворять следующим основным требованиям:
 - а) быстро включаться и отключаться от электросети (но не самопроизвольно);
 - б) быть безопасными в работе и иметь недоступные для случайного прикосновения токоведущие части;
 - в) подключаться к розетке оборудованной дополнительной заземляющей жилой или иметь заземленный корпус.

Перед началом работы на ПЭВМ необходимо проверить:

1. Состояние сетевого кабеля, целостность изоляции, отсутствие излома жил, надежность крепления сетевой вилки.
2. Исправность заземления, защитных отключающих устройств.

При обнаружении каких-либо неисправностей работа на ПЭВМ должна быть немедленно прекращена и об этом доложено преподавателю или инженеру (технику) лаборатории.

Во время работы на ПЭВМ запрещается:

1. Начинать работу на ПЭВМ без прохождения инструктажа по мерам безопасности при работе с ПЭВМ.
2. Включать ПЭВМ без разрешения преподавателя.
3. Самостоятельно (без указания преподавателя) изменять что-либо в схеме или удалять какие-либо файлы в директории с установленной программой.

4. Без разрешения заведующего лаборатории, инженера или техника переносить с места на место системные блоки, мониторы, другие комплектующие ПЭВМ и периферийные устройства.
5. Снимать защитный кожух системного блока и монитора и производить самим какой-либо ремонт (как ПЭВМ, так и другого оборудования, разного рода кабелей и т.п.).
6. Держать сетевой кабель, касаться открытых токонесущих элементов, касаться одновременно корпуса ПЭВМ (металлических частей периферийных устройств) и заземляющего провода.
7. Подключать к работающей ПЭВМ и отключать от нее периферийные устройства, проверять надежность подключенных кабелей.
8. Касаться сетевых терминаторов и коннекторов, вынимать их из разъемов сетевых карт.
9. Разбирать силовые розетки, помещать в них посторонние предметы.

Перечень лицензионного программного обеспечения, используемого на лекционных и семинарских занятиях: Microsoft Office; Adobe Acrobat; Adobe Master Collection CS4; Windows 10 Pro; AutoCAD 2010 Student; Archicad 21 Rus Student; SPSS Statistics 22; Microsoft Share Point 2010; SPSS Statistics 25; Microsoft Office 2013; ОС «Альт Образование» 8; Kaspersky Endpoint Security; Visual Studio 2019; Adobe Creative Cloud.

Состав программного обеспечения (ПО), современных профессиональных баз данных (БД) и информационно-справочных систем (ИСС) (2017 г.)

1. Перечень ПО

Таблица 1

№п/п	Наименование ПО	Производитель	Способ распространения (лицензионное или свободно распространяемое)
1	Adobe Master Collection CS4	Adobe	лицензионное
2	Microsoft Office 2010	Microsoft	лицензионное
3	Windows 7 Pro	Microsoft	лицензионное
7	Microsoft Share Point 2010	Microsoft	лицензионное
9	Microsoft Office 2013	Microsoft	лицензионное
11	Kaspersky Endpoint Security	Kaspersky	лицензионное

2. Перечень БД и ИСС

Таблица 2

№п/п	Наименование
	Международные реферативные наукометрические БД, доступные в рамках национальной подписки в 2017 г. Web of Science Scopus
	Профессиональные полнотекстовые БД, доступные в рамках нацио-

	нальной подписки в 2017 г. Журналы Oxford University Press ProQuest Dissertation & Theses Global SAGE Journals Журналы Taylor and Francis
	Профессиональные полнотекстовые БД JSTOR Издания по общественным и гуманитарным наукам
	Компьютерные справочные правовые системы Консультант Плюс, Гарант

Состав программного обеспечения (ПО), современных профессиональных баз данных (БД) и информационно-справочные систем (ИСС) (2018 г.)

1. Перечень ПО

Таблица 1

№п/п	Наименование ПО	Производитель	Способ распространения (лицензионное или свободно распространяемое)
1	Adobe Master Collection CS4	Adobe	лицензионное
2	Microsoft Office 2010	Microsoft	лицензионное
3	Windows 7 Pro	Microsoft	лицензионное
7	Microsoft Share Point 2010	Microsoft	лицензионное
9	Microsoft Office 2013	Microsoft	лицензионное
11	Kaspersky Endpoint Security	Kaspersky	лицензионное

2. Перечень БД и ИСС

Таблица 2

№п/п	Наименование
	Международные реферативные наукометрические БД, доступные в рамках национальной подписки в 2018 г. Web of Science Scopus
	Профессиональные полнотекстовые БД, доступные в рамках национальной подписки в 2018 г. Журналы Oxford University Press ProQuest Dissertation & Theses Global SAGE Journals Журналы Taylor and Francis
	Профессиональные полнотекстовые БД JSTOR Издания по общественным и гуманитарным наукам
	Компьютерные справочные правовые системы Консультант Плюс, Гарант

Состав программного обеспечения (ПО), современных профессиональных баз данных (БД) и информационно-справочные систем (ИСС) (2019 г.)

1. Перечень ПО

Таблица 1

№п/п	Наименование ПО	Производитель	Способ распространения (лицензионное или свободно распространяемое)
1	Adobe Master Collection CS4	Adobe	лицензионное
2	Microsoft Office 2010	Microsoft	лицензионное
3	Windows 7 Pro	Microsoft	лицензионное
7	Microsoft Share Point 2010	Microsoft	лицензионное
9	Microsoft Office 2013	Microsoft	лицензионное
12	Windows 10 Pro	Microsoft	лицензионное
13	Kaspersky Endpoint Security	Kaspersky	лицензионное

2. Перечень БД и ИСС

Таблица 2

№п/п	Наименование
	Международные реферативные наукометрические БД, доступные в рамках национальной подписки в 2019 г. Web of Science Scopus
	Профессиональные полнотекстовые БД, доступные в рамках национальной подписки в 2019 г. Журналы Cambridge University Press ProQuest Dissertation & Theses Global SAGE Journals Журналы Taylor and Francis Электронные издания издательства Springer
	Профессиональные полнотекстовые БД JSTOR Издания по общественным и гуманитарным наукам
	Компьютерные справочные правовые системы Консультант Плюс, Гарант

8. Обеспечение образовательного процесса для лиц с ограниченными возможностями здоровья

В ходе реализации дисциплины используются следующие дополнительные

методы обучения, текущего контроля успеваемости и промежуточной аттестации обучающихся в зависимости от их индивидуальных особенностей:

- для слепых и слабовидящих:
 - лекции оформляются в виде электронного документа, доступного с помощью компьютера со специализированным программным обеспечением;
 - письменные задания выполняются на компьютере со специализированным программным обеспечением, или могут быть заменены устным ответом;
 - обеспечивается индивидуальное равномерное освещение не менее 300 люкс;
 - для выполнения задания при необходимости предоставляется увеличивающее устройство; возможно также использование собственных увеличивающих устройств;
 - письменные задания оформляются увеличенным шрифтом;
 - экзамен и зачёт проводятся в устной форме или выполняются в письменной форме на компьютере.
- для глухих и слабослышащих:
 - лекции оформляются в виде электронного документа, либо предоставляется звукоусиливающая аппаратура индивидуального пользования;
 - письменные задания выполняются на компьютере в письменной форме;
 - экзамен и зачёт проводятся в письменной форме на компьютере; возможно проведение в форме тестирования.
- для лиц с нарушениями опорно-двигательного аппарата:
 - лекции оформляются в виде электронного документа, доступного с помощью компьютера со специализированным программным обеспечением;
 - письменные задания выполняются на компьютере со специализированным программным обеспечением;
 - экзамен проводится в устной форме или в письменной форме на компьютере.

При необходимости предусматривается увеличение времени для подготовки ответа.

Процедура проведения промежуточной аттестации для обучающихся устанавливается с учётом их индивидуальных психофизических особенностей. Промежуточная аттестация может проводиться в несколько этапов.

При проведении процедуры оценивания результатов обучения предусматривается использование технических средств, необходимых в связи с индивидуальными особенностями обучающихся. Эти средства могут быть предоставлены университетом, или могут использоваться собственные технические средства.

Проведение процедуры оценивания результатов обучения допускается с использованием дистанционных образовательных технологий.

Обеспечивается доступ к информационным и библиографическим ресурсам в сети Интернет для каждого обучающегося в формах, адаптированных к ограничениям их здоровья и восприятия информации:

- для слепых и слабовидящих:
 - в печатной форме увеличенным шрифтом;

- в форме электронного документа;
- в форме аудиофайла.
- для глухих и слабослышащих:
 - в печатной форме;
 - в форме электронного документа.
- для обучающихся с нарушениями опорно-двигательного аппарата:
 - в печатной форме;
 - в форме электронного документа;
 - в форме аудиофайла.

Учебные аудитории для всех видов контактной и самостоятельной работы, научная библиотека и иные помещения для обучения оснащены специальным оборудованием и учебными местами с техническими средствами обучения:

- для слепых и слабовидящих:
 - устройством для сканирования и чтения с камерой SARA CE;
 - дисплеем Брайля PAC Mate 20;
 - принтером Брайля EmBraille ViewPlus;
- для глухих и слабослышащих:
 - автоматизированным рабочим местом для людей с нарушением слуха и слабослышащих;
 - акустический усилитель и колонки;
- для обучающихся с нарушениями опорно-двигательного аппарата:
 - передвижными, регулируемыми эргономическими партами СИ-1;
 - компьютерной техникой со специальным программным обеспечением.

9. Методические материалы

Успешное освоение дисциплины студентом определяется, несколькими факторами: посещение аудиторных занятий, подготовка и выполнение домашних заданий, практических и контрольных работ, своевременное выполнение запланированных форм отчетности.

9.1. Планы лабораторных занятий

Самостоятельные занятия направлены на закрепление полученных навыков и для приобретения новых теоретических и фактических знаний, выполняется в читальном зале библиотеки и в домашних условиях, подкрепляется учебно-методическим и информационным обеспечением (учебники, учебно-методические пособия, конспекты лекций).

Самостоятельные занятия выполняется с использованием ПК в домашних условиях, либо в библиотеке института по специальным заданиям в соответствии с методическими материалами, выданными преподавателем. Самостоятельные занятия включает отработку навыков анализа ситуации, создание модели ситуации, которая используется в данном конкретном методе, и решение задачи, также к самостоятельной работе относится выполнение заданий по пройденному материалу. Подготовка по темам пропущенных занятий.

Начиная с первого занятия, преподаватель объявляет студентам тему следующего занятия и список литературы. Студент должен ознакомиться с предложенными источниками, в таком случае он на следующем занятии будет готов к восприятию нового материала.

Студент для самостоятельной работы должен иметь программу курса, вопросы к экзамену, список основной и дополнительной литературы по курсу.

После каждого занятия, перед следующим, студент должен ознакомиться с пройденным материалом. При возникновении вопросов или непонимания, студент должен изучить рекомендованную и дополнительную литературу по курсу.

Процесс изучения дисциплины предусматривает выполнение обучающимися следующих видов самостоятельной работы:

- подготовка к лекциям,
- практическим занятиям, устным опросам,
- выполнение письменных работ,
- подготовка к итоговой аттестации.

Вопросы для самостоятельной проработки и самоконтроля

Раздел № 1 Методологические аспекты информационной безопасности (ИБ) и защиты информации (ЗИ)

- 1 Освоение основных терминов и определений, понятий в области ИБ и ЗИ.
- 2 Связь ИБ с информатизацией общества.
- 3 Необходимость и значение нормативно-правового определения основных понятий.
- 4 Классификация угроз ИБ, каналов НСД к информации в ИС. Подготовка к тестированию.
- 5 Какие объекты защиты в информационных системах (ИС).
- 6 Основные источники угроз для ИС.
- 7 Характерные угрозы для информационных ресурсов (ИР).
- 8 Подготовка домашней работы по заданию преподавателя.

Раздел № 2 Информационная безопасность. Меры обеспечения информационной безопасности

1. Понятие и назначение стандартов.
2. Виды стандартов и критерии оценки состояния информационной безопасности.
3. Российские нормативно-правовые акты в области ИБ.
4. Базовые принципы защиты информации от несанкционированного доступа (НСД) в соответствии с нормативно-правовыми документами
5. Основные группы классов защищенности ИС.
6. Основные разделы и содержание политики ИБ.
7. Основные разделы и содержание программы ИБ.
8. Базовые инструментальные средства для анализа рисков.
9. Стратегии управления рисками.

10. Минимизация привилегий и распределение обязанностей между персоналом, как основной принцип исключения от случайных ошибок и реализации преднамеренных угроз
11. Основные требования к персоналу по поддержанию работоспособности. ИС,
12. Основные правила по исключении дестабилизирующих факторов нарушения состояния ИБ
13. Действия персонала по минимизации ущерба при планирование восстановительных работ
14. Основные проблемы в построении СЗИ, связанных с развитием информационных технологий.
15. Перечислите принципы архитектурной безопасности для обеспечения конфиденциальности ИР.
16. Основные группы методов аутентификации.
17. Особенности протоколирования и аудита. ИБ.
18. Симметричные и ассиметричные криптосистемы.
19. Компьютерная стеганография.
20. Основные классы межсетевых экранов.
21. Подготовка домашней работы по заданию преподавателя.

Раздел 3. Система защиты информации

1. Структура государственной системы защиты информации, задачи органов законодательной, исполнительной и судебной власти по созданию условий по обеспечению информационной безопасности.
2. Назовите государственные органы по контролю и надзору за обеспечением защиты государственной тайны и конфиденциальной информации их задачи и функции.
3. Классификация нарушителей по возможности доступа к объекту (предмету) защиты, степени подготовки и оснащенности средствами взлома, обхода средств защиты информации.
4. Возможные причины, условия и обстоятельства, создающие предпосылки для свершения преступлений (правонарушений).
5. Что понимается под комплексным подходом к защите информации.
6. Что понимается под системным подходом к защите информации.
7. Какие исходные данные для построения системы защиты информации.
8. Структура системы защиты информации на предприятиях.
9. Перечислите этапы и перечень работ по созданию системы защиты информации.
10. подготовка домашней работы по заданию преподавателя.

Раздел 4. Контроль и ответственность по обеспечению информационной безопасности и защиты информации

1. Основные положения по осуществлению контроля. Цели, задачи, принципы контроля.
2. Основные мероприятия по осуществлению контроля.
3. Проверка (контроль) наличия конфиденциальных документов и иных носителей конфиденциальных сведений.
4. Проведение служебного расследования по фактам нарушения требований режима конфиденциальности.
5. Понятие и виды юридической ответственности за нарушение правовых норм по защите информации.
6. Меры дисциплинарной ответственности согласно Трудового кодекса РФ.

7. Административная ответственность за правонарушения в области защиты информации.
8. Уголовная ответственность за правонарушения и преступления в области конфиденциальной информации.
9. Уголовная ответственность за правонарушения и преступления в области государственной тайны.
10. Подготовка домашней работы по заданию преподавателя.

Методические указания по организации и проведению лабораторных работ

Лабораторная работа № 1. Разработка клиент-серверного приложения в Delphi.

Цель работы: Изучить современные средства создания клиент-серверных приложений в системе Delphi. Научиться практической работе по организации и решению задач информационной безопасности в сети.

Задание на лабораторную работу

1. Изучить теоретический материал по данной лабораторной работе.
2. Ознакомиться с указаниями по программированию на языке Pascal в среде Delphi.
3. Разработать программный комплекс, представляющий собой клиент-серверное приложение в среде Delphi, осуществляющее передачу данных между двумя хостами в сети.
4. Выполнить пробное шифрование/расшифровку данных, передаваемых по сети в рамках компьютерного класса. Вставить в отчет полученные данные, описать методику выполнения задания.
5. Ответить на контрольные вопросы в конце задания.

Теоретический материал.

Рассмотрим процедуры создания приложений для обмена сообщениями в сети по протоколам TCP/IP.

Разработка TCP-сервера в Delphi.

1. Нанесем на форму Delphi компоненту TidServer с вкладки IndyServer.
2. В его свойстве Bindings укажем IP-адрес данного компьютера и номер порта, на котором сервер будет ожидать вызова от клиента (номер порта – произвольное число от 1 до 65535, но желательно использовать номера выше 1024, т. к. порты с меньшими номерами зарезервированы для стандартных служб),
3. В свойстве MaxConnections укажите 5 (максимальное число соединений к серверу), в свойство Default Port запишите значение порта по умолчанию, а в свойство Active запишите true.
4. Добавьте на форму элемент типа TМемо для вывода в него сообщений, полученных от клиента,

5. При вызове клиента вырабатывается событие OnExecute элемента IdServer1. Для его обработки откройте вкладку Events Инспектора объектов и щелкните дважды в поле процедуры OnExecute.

6. В открывшейся процедуре введите следующий код:

```
Procedure TForm1.IdTCTServer1Execute(Athread:TidPeerConnection);  
Begin  
with Athread. Connection do  
begin  
Memo1.Lines. Add(CurrentReadBuffer);  
Writeln('Сообщение получено');  
Disconnect;  
end;  
End;
```

Приложение ТСТ-клиент в Delphi.

1. Нанесите на форму элемент TidTCPClient с панели IndyClient, два элемента типа Tedit для ввода сообщений серверу и получения ответа, и кнопку TButton.

2. В свойстве Host элемента TidTCPClient укажите IP-адрес сервера, а в свойстве Port задайте номер порта (тот же, что у сервера).

3. Щелкните дважды по элементу Button1 и в появившемся окне введите следующий код:

```
Procedure TForm1.Button1click(Sender: TObject);  
Begin  
IdTCPClient1.Connect;  
IdTCPClient1.Writeln(Edit1.Text);  
Edit2.Text:= IdTCPClient1.ReadLn;  
IdTCPClient1.Disconnect;  
End;
```

4. Добавьте код функции MD5, взятый из описания лабораторной работы №3.

5. Запустите оба приложения и протестируйте полученную программу.

Контрольные вопросы

1. На какой вкладке Delphi находятся компоненты для создания клиент-серверного приложения?

2. Какие основные свойства надо установить в компоненте Indy Server?

3. Какие основные свойства надо установить в компоненте Indy Client?

4. Какой протокол используют компоненты Indy Server и Indy Client для установления связи по локальной сети? Можно ли использовать приложение в сети Интернет?

Лабораторная работа № 2. Решение в локальной сети задачи аутентификация пользователей.

Цель. Ознакомиться с основными алгоритмами аутентификации пользователей в сети, электронной подписи, сертификации. Разработать комплекс программ в Delphi для пересылки и проверки идентификаторов пользователей, решения задачи распределения секретного ключа, идентификации посланий на основе электронно - цифровой подписи и сертификатов.

Программно-аппаратные средства. Компьютерная лаборатория, состоящая из компьютеров, соединенных в локальную сеть, пакет Delphi 7 (Delphi 2005).

Задание на лабораторную работу

1. Изучить теоретический материал по данной лабораторной работе.
2. Разработать программный комплекс в среде Delphi генерации параметров метода RSA и пересылки (публикации) открытого ключа в сети.
3. Реализовать алгоритм генерации электронно - цифровой подписи с использование закрытого ключа метода RSA и функции хеширования MD5.
4. Реализовать алгоритм проверки электронно - цифровой подписи с использование открытого ключа метода RSA и функции хеширования MD5.
5. Выполнить пробную пересылку данных в рамках локальной сети компьютерного класса, снабженных ЭЦП. Вставить в отчет полученные данные, описать методику выполнения задания.
6. Ответить на контрольные вопросы в конце задания.

Теоретический материал.

Одной из наиболее важных служб безопасности является аутентификация. Аутентификация – это подтверждение пользователем информационных услуг своего идентификатора. Аутентификация выполняется с помощью разных методов, из которых простейшим является предъявления пользователем серверу секретного слова – пароля, известного только пользователю и серверу.

Хеш-функции

Хеш-функции играют в информационной защите важную роль, создавая для электронного документа его «моментальный снимок» и тем самым защищая документ от дальнейшей модификации или подмены.

В широком смысле функцией хеширования называется функция H, удовлетворяющая следующим основным свойствам:

1. Хеш-функция H может применяться к блоку данных любой длины.
2. Хеш-функция H создает выход фиксированной длины (равно, например, 128 бит для классической функции хеширования MD5, и 160 бит для функции SHA1).
3. $H(M)$ вычисляется относительно быстро (за полиномиальное время от длины сообщения M).
4. Для любого данного значения хеш-кода h вычислительно невозможно найти M такое, что $H(M) = h$.
5. Для любого данного x вычислительно невозможно найти y x , что $H(y) = H(x)$.
6. Вычислительно невозможно найти произвольную пару (x, y) такую, что $H(y) = H(x)$.

Термин вычислительно невозможно означает здесь, что в настоящее время решение этой задачи либо требует слишком большого интервала времени (например, более сотни лет), либо использования слишком больших вычислительных ресурсов, чтобы решение задачи имело смысл.

Первые три свойства требуют, чтобы хеш-функция создавала хеш-код для любого сообщения. Четвертое свойство определяет требование односторонности хеш-функции: легко создать хеш-код по данному сообщению, но невозможно восстановить сообщение по данному хеш-коду.

Схемы аутентификации.

Поскольку при передаче данных по сети никто не застрахован от возможности чтения данных на промежуточных узлах, то передача пароля по сети в открытом виде является опасным. Поэтому для надежной аутентификации и сохранения пароля от взлома используются разные схемы сетевой аутентификации. Здесь мы рассмотрим следующие три схемы:

Схема аутентификации на основе слова-вызова и хеш-свертки.

В этой схеме пользователь зарегистрировавшись на сервере, получает секретный ключ P , который сохраняется также на сервере. При выходе на связь пользователь посылает сначала свой идентификатор. Получив идентификатор, сервер проверяет наличие такого пользователя по своей базе данных и затем возвращает пользователю случайное большое число N (обычно длины 16 байт), называемое словом-вызовом. Пользователь, получив это число, формирует пару $\langle N, P, TS \rangle$, где P обозначает пароль пользователя, TS – текущий момент времени (Time Stamp), подвергает ее хеш-преобразованию и отправляет полученное значение $h = h(\langle N, P \rangle)$ серверу. Сервер, получив свертку h , извлекает из базы данных пароль пользователя, выполняет то же преобразование $h(\langle N, P \rangle)$ и сравнивает два полученных значения h . Если они совпали, то процедура аутентификация считается успешной.

Схема аутентификации на основе электронной подписи (ЭП).

В этой схеме пользователь зарегистрировавшись на сервере, получает пару открытый/секретный ключ P . Открытый ключ сохраняется также на сервере. При выходе на связь пользователь формирует набор $\langle Id, M, Ts \rangle$, где Id обозначает идентификатор пользователя, M – сообщение пользователя, Ts – метка времени (Time Stamp), подвергает его хеш-преобразованию $h = h(\langle Id, M, Ts \rangle)$ и шифрует закрытым ключом $EncK_z(h)$. Полученный код называется электронно-цифровой подписью и служит для подтверждения неизменности сообщения и проверки авторства послания. Электронно-цифровая подпись $EncK_o(h(\langle Id, M, Ts \rangle))$ прикладывается к исходному сообщению $\langle Id, M, Ts \rangle$ и отправляется на сервер.

Сервер, получив пакет, расшифровывает ЭЦП, извлекая свертку $h(\langle Id, M, Ts \rangle)$, параллельно вычисляет такую же свертку $h = h(\langle Id, M, Ts \rangle)$, используя те же исходные данные и хеш функцию, и сравнивает два полученных значения h . Если они совпали, то процедура аутентификация считается успешной. Временная метка Ts выполняет роль сеансового ключа для предотвращения атак воспроизведения.

Использование хеш-функции в этом методе не является обязательным и служит лишь для уменьшения объема вычислений для шифрования и сокращения сетевого трафика.

Электронно-цифровая подпись может быть сформирована на основе различных методов двухключевой криптографии, например, RSA, Эль-Гамала, эллиптических кривых.

Схема аутентификации на основе сертификата.

Данная схема предполагает наличие третьей стороны, называемой УЦ – удостоверяющим центром или ЦС – центром сертификации, которая выдает удостоверения (сертификаты) всем участникам сетевого домена, входящего в зону действия данного ЦС. При регистрации нового пользователя или сервера в домене ЦС выдает новому участнику сертификат, состоящий из открытой части, содержащий такие данные как:

1. Идентификатор владельца сертификата,
2. Адрес владельца сертификата,
3. Открытый ключ владельца сертификата,
4. Категория владельца сертификата (например, пользователь с ограниченными полномочиями или администратор проекта).
5. Наименование ЦС и его адрес,
6. Алгоритмы, используемые для генерации ключей и формирования ЭЦП, и их версии, и закрытой части, содержащий ту же информацию, закреплённой электронно-цифровой подписью ЦС (т. е. подвергнутого хеш - преобразованию и последующему шифрованию с помощью закрытого ключа ЦС).

Обе части выдаются соискателю в электронном виде в виде одного файла. Закрытая часть служит для того, чтобы нельзя было подделать сертификат.

Кроме того, соискатель получает отдельно закрытый ключ, соответствующий открытому ключу, находящемуся в сертификате, который соискатель обязуется хранить в секрете.

Кроме того, открытая часть сертификата может выдана в виде бумажного документа, подтвержденного печатью ЦС.

При обмене сообщения каждый участник сопровождает свое послание меткой времени, электронно-цифровой подписью, сформированной на основе своего закрытого ключа, и сертификатом, выданным ему ЦС. Сертификат здесь служит для удостоверения ЭЦП отправителя: получатель подписывает своим закрытым ключом послания, а получатель расшифровывает ЭЦП, используя открытый ключ отправителя, извлеченный из сертификата. Подлинность сертификата подтверждается электронно-цифровой подписью ЦС, которая может быть проверена с помощью расшифровки закрытой части сертификата с использованием открытого ключа ЦС, который является общедоступным.

Программирование хеш-функций в Delphi

Система Delphi обращается к встроенным средствам операционной системы Windows для программирования различных функций хеширования, методов шифрования с использованием классической и двухключевой криптографии. Большинство этих средств содержится в библиотеках `advapi32.dll` и `crypt32.dll`, которые должны быть подключены к проекту Delphi. Для этого в проект приложения надо добавить модуль `Wcrypt2.pas`, который можно скачать по адресу

<http://www.delphikingdom.com/zip/headerCryptoAPI.rar>. Как воспользоваться этим модулем в проекте Delphi можно прочитать в статье Ю. Спектора

<http://www.delphikingdom.com/asp/viewitem.asp?catalogID=1271>.

Если нет необходимости использовать все возможности этих библиотек, то можно воспользоваться готовой программой для хеш-функции MD5 (см. прил. в конце).

Указания к выполнению лабораторной работе.

Лабораторная работа 4 состоит из двух частей, каждая из которых выполняется в одной форме Delphi.

В первой части следует разработать клиент-серверное приложение для удаленной аутентификации пользователей на компьютере-сервере согласно номеру своего варианта. Для этого используйте разработку, выполненную в лабораторной работе 2.

Во второй части надо выполнить написать приложение, представляющее работу Центра Сертификации X.509 по выдаче сертификатов X.509 другим пользователям сети по их запросам.

Варианты заданий

Четные варианты. Разработать приложение, осуществляющее аутентификацию пользователей на основе слова-вызова.

Нечетные варианты. Разработать приложение, осуществляющее аутентификацию пользователей на основе электронно-цифровой подписи, генерируемой с помощью метода RSA.

Контрольные вопросы

1. Что такое аутентификация? Перечислите основные методы аутентификации.
2. Что такое хеш-преобразование? Перечислите основные свойства хеш-функций.
3. В чем заключается аутентификация на основе слова-вызова?
4. Что такое электронно-цифровая подпись? Как она формируется?
5. Как выполняется проверка послания, подписанного ЭЦП?
6. Что такое сертификация X.509? Каковы преимущества имеет аутентификация на основе сертификатов по сравнению с другими видами сертификации?
7. Что входит в состав сертификата?
8. Какие основные функции выполняет Центр Сертификации X.509?
9. Сколько различных ключей используется в процедуре аутентификация на основе сертификатов, и каким образом распространяются эти ключи?
10. Каким образом осуществляется проверка подлинности сертификата?

Литература:

1. А. В.Беляев. "Методы и средства защиты информации" (курс лекций). <http://www.citforum.ru/internet/infsecure/index.shtml>
2. А. Володин. «Кто заверит ЭЦП», журнал «Банковские системы», ноябрь 2000, <http://www.bizcom.ru/system/2000-11/04.html>
3. Т. Илонен. Введение в криптографию (Ylonen Tatu. Introduction to Cryptography), <http://www.ssl.stu.neva.ru/psw/crypto/intro.html>
4. Ш. Т. Ишмухаметов. Технологии защиты информации в сети, Казань, 2008, 91 с. <http://depositfiles.com/files/e9zxcqos9>
5. Н. Коблиц. Теория чисел и криптография, М.:, ТВР, 2001 http://gabro.ge/biblio/0708/0081/file/Cryptography/Koblic_-_Teoriya_Chisel_i_Cryptografiya.rar
6. О. Р. Лапоница. Криптографические основы безопасности, курс Интернет-университета, <http://www.intuit.ru/department/security/networksec>
7. Р. Лидл, Г. Нидеррайтер. Конечные поля, в 2 т., пер. с англ., М.: Мир, 1998, 438 с.
8. А. А. Молдовян, Н. А. Молдовян, Введение в криптосистемы с открытым ключом, БХВ-Петербург, 2005, с. 286 http://cyberdoc.nnm.ru/vvedenie_v_kriptosistemy_s_otkryтым_klyuchom

9. А. Г.Ростовцев, Е. Б.Маховенко. Теоретическая криптография. – СПб.: АНО, ПО “Профессионал”, 2005, <http://bookpedia.ru/index.php?newsid=1265>
10. Г. Семенов. «Цифровая подпись. Эллиптические кривые».
<http://www.morepc.ru/security/crypt/os200207010.html?print>
11. Брюс Шнайер. Прикладная криптография, 2-е издание: протоколы, алгоритмы и исходные тексты на языке С, http://www.ssl.stu.neva.ru/psw/crypto/appl_rus/appl_cryp.htm
12. Dr. Michael Ganley, Thales eSecurity Ltd. Метод эллиптических кривых, http://www.racal.ru/rsp/elliptic_curve_cryptography.htm
13. В. М.Фомичев. Дискретная математика и криптология, Диалог-МИФИ, 2003, 399 с.
14. Сайт Криптографический ликбез - <http://www.ssl.stu.neva.ru/psw/crypto.html>
15. Jovan Dj. Golic. Cryptanalysis of Alleged A5 Stream Cipher, Beograd, Yugoslavia, <http://jya.com/a5-hack.htm>
16. Ю. Спектор. Использование инструментов криптографии в Delphi-приложениях, <http://www.delphikingdom.com/asp/viewitem.asp?catalogID=1271>

9.2. Методические рекомендации по подготовке письменных работ (рефератов, докладов)

Реферат, доклад – продукт самостоятельной работы студента, представляющий собой написание учебной работы и публичное выступление по представлению полученных результатов решения определенной учебно-практической, учебно-исследовательской или научной темы.

Примерный перечень тем рефератов, докладов

1. Основные методики, используемые для оценки рисков.
2. Процедура формирования электронной подписи.
3. Основные каналы несанкционированного доступа (НСД) к информации при ее обработке с использованием технических средств.
4. Методы, способы несанкционированного доступа (НСД) к информации при ее обработке на СВТ (АС).
5. Основные уровни обеспечения информационной безопасности.
6. Классификация угроз, источников угроз информационной безопасности при обработке информации с использованием технических средств.
7. Основные положения ФЗ «Об информации, информационных технологиях и о защите информации».
8. Концептуальные нормативно-правовые акты России в области защиты информации.

9. Роль в России Межведомственной комиссии по защите государственной тайны в формировании перечня сведений, составляющих государственную тайну.
10. Виды и классификация компьютерных преступлений.
11. Виды компьютерных преступлений, методы противодействия компьютерным преступлениям.
12. Политика информационной безопасности, основные положения и этапы её разработки.
13. Программа информационной безопасности, основные положения и этапы её разработки.
14. Основные угрозы компьютерным системам.
15. Методики оценки рисков для информационных систем.
16. Стандарты в области разработки политики информационной безопасности.
17. Инструментальные средства для анализа рисков и управления ими.
18. Законодательный уровень информационной безопасности, основные нормативно-правовые документы необходимые для обеспечения безопасности информации на предприятии.
19. Административный уровень информационной безопасности, политика и программа информационной безопасности.
20. Административный уровень информационной безопасности, анализ, учет и управления рисками.
21. Процедурный уровень информационной безопасности, назначение, цели и решаемые задачи.
22. Программно-технический уровень информационной безопасности, назначение, цели и решаемые задачи,
23. Принципы построения архитектурной безопасности информационных систем.
24. Основные группы процедурных мер по обеспечению информационной безопасности.
25. Базовые направления поддержки работоспособности информационных систем.
26. Основные сервисы программных средств защиты информации в информационных системах.
27. Базовые группы методов аутентификации.
28. Основные правила парольной защиты в компьютерных системах.
29. Биометрические системы идентификации пользователей.
30. Основные виды управления доступом к информации.
31. Классификация программ-вирусов.
32. Базовые виды антивирусных программ.
33. Классификация вредоносных программ.
34. Основные свойства антивирусного программного продукта Лаборатории Касперского.

35. Классификация методов криптографического преобразования данных.
36. Блочное и потоковое шифрование.
37. Основные методы шифрования данных.
38. Базовые криптографические стандарты.
39. Симметричные и ассиметричные криптосистемы.
40. Стеганографические системы при передаче информации по каналам связи .
41. Базовые ресурсы информационных систем, подлежащих защите.
42. Основные принципы архитектурной безопасности информационных систем.
43. Сервисы безопасности для реализации защитных функций вычислительной сети.
44. Иерархия сервисов безопасности в информационных телекоммуникационных системах (ИТС).
45. Юридическая ответственность за нарушение правовых норм по защите информации.
46. Меры дисциплинарной за нарушение правовых норм по защите информации.
47. Административная ответственность за правонарушения в области защиты информации.
48. Уголовная ответственность за правонарушения и преступления в области конфиденциальной информации.

АННОТАЦИЯ ДИСЦИПЛИНЫ

Дисциплина «Информационная безопасность и защита информации» является частью обязательного цикла (блока) дисциплин цикла учебного плана по направлению подготовки бакалавров 46.03.02 «Документоведение и архивоведение».

Дисциплина реализуется на факультетах Документоведения и технотронных архивов и архивного дела кафедрой Комплексной защиты информации ИИНТБ РГГУ.

Содержание дисциплины охватывает круг вопросов, связанных с информационной безопасностью и защитой информации в Российской Федерации.

Цель дисциплины:

изучение теоретических и прикладных вопросов информационной безопасности и защиты информации в сфере документооборота и архивного дела в Российской Федерации.

Задачи дисциплины:

изучить исторические этапы развития информационной безопасности и защиты информации;

освоить терминологию и понятийный аппарат в области информационной безопасности и защиты информации;

изучить нормативно-правовую базу, регулирующую сферу информационной безопасности и защиты информации; изучить основные средства и методы обеспечения информационной безопасности;

научить определять угрозы, уязвимости и риски информационной безопасности; обучить навыкам защиты информации;

научить применять полученные знания и навыки по информационной безопасности и защите информации в сфере документооборота и архивного дела.

Выпускник, освоивший программу бакалавриата, должен обладать:

общекультурными компетенциями:

– способностью использовать теоретические знания и методы исследования на практике (ОПК -1);

– владением базовыми знаниями в области информационных технологий (программные продукты, используемые в управлении документами, системы электронного документооборота, технологии сканирования документов) (ОПК-2);

В результате освоения дисциплины обучающийся должен:

Знать:

- историю, современное состояние, проблемы и тенденции развития систем информационной безопасности и защиты информации
- нормативно-правовую базу обеспечения информационной безопасности и защиты информации
- систему органов власти, определяющих и реализующих государственную политику в области информационной безопасности и защиты информации
- систему документационного обеспечения информационной безопасности и защиты информации
- место и роль информационной безопасности и защиты информации в области документооборота и архивного дела
- методы и средства обеспечения информационной безопасности и защиты информации

Уметь:

- анализировать проблемы информационной безопасности и защиты информации в системах документооборота и архивном деле
- применять отечественные и зарубежные стандарты в области информационной безопасности и защиты информации
- определять угрозы, уязвимости и риски информационной безопасности
- разрабатывать комплекс мер по обеспечению информационной безопасности и защиты информации в сфере документооборота и архивного дела

Владеть:

- терминологией и понятийным аппаратом в области информационной безопасности и защиты информации
- навыками использования методов и средств обеспечения информационной безопасности и защиты информации
- навыками разработки документационного обеспечения информационной безопасности и защиты информации

Рабочей программой предусмотрены следующие виды контроля: текущий контроль успеваемости в форме обзора, доклада, реферата, контрольной работы, опроса.

Итоговая аттестация в форме зачета. Общая трудоемкость освоения дисциплины составляет: 2 зачетных единицы, 72 часа.

ЛИСТ ИЗМЕНЕНИЙ

№	Текст актуализации или прилагаемый к РПД документ, содержащий изменения	Дата	№ протокола
3	Обновлена основная и дополнительная литература	29.06.2017	№6
4	Обновлена структура дисциплины для очной форм обучения		
5	Обновлена основная и дополнительная литература	26.06.2018	№5
6	Обновлена структура дисциплины для очной форм обучения		
7	Обновлен состав программного обеспечения (ПО), современных профессиональных баз данных (БД) и информационно-справочные систем (ИСС) Приложение 2.1.	22.06.2020	№10

Приложение 2.1.

Состав программного обеспечения (ПО), современных профессиональных баз данных (БД) и информационно-справочные систем (ИСС) (2020 г.)

1. Перечень ПО

№ п/п	Наименование ПО	Производитель	Способ распространения (лицензионное или свободно распространяемое)
1.	Adobe Master Collection CS4	Adobe	лицензионное
2.	Microsoft Office 2010	Microsoft	лицензионное
3.	Windows 7 Pro	Microsoft	лицензионное
4.	Microsoft Office 2013	Microsoft	лицензионное
5.	Windows 10 Pro	Microsoft	лицензионное
6.	Kaspersky Endpoint Security	Kaspersky	лицензионное
7.	Microsoft Office 2016	Microsoft	Лицензионное
8.	Zoom	Zoom	лицензионное

2. Перечень БД и ИСС

№ п/п	Наименование
1	Международные реферативные наукометрические БД, доступные в рамках национальной подписки в 2020 г. Web of Science Scopus
2	Профессиональные полнотекстовые БД, доступные в рамках национальной подписки в 2020 г. Журналы Cambridge University Press ProQuest Dissertation & Theses Global SAGE Journals Журналы Taylor and Francis
3	Профессиональные полнотекстовые БД JSTOR Издания по общественным и гуманитарным наукам Электронная библиотека Grebennikon.ru
4	Компьютерные справочные правовые системы Консультант Плюс, Гарант

